

Algebra

XX

May 27, 2019

1 Group

1.1 Groups

Definition 1.1 (Group). A group $(G, *)$ is a set G together with a law of composition $(G * G \rightarrow G)$ which is associative and has an identity element, and such that every element of G has an inverse. That is, $(G, *)$ satisfies

1. (Closure) $\forall a, b \in G, a * b \in G$.
2. (Identity) $\exists e, \text{ s.t. } \forall g \in G, g * e = e * g = g$.
3. (Inverse) $\forall g \in G, \exists g^{-1} \text{ in } G, \text{ s.t. } g * g^{-1} = e$.
4. (Associativity) $\forall a, b, c \in G, (a * b) * c = a * (b * c)$.

Remark 1.1. Identity e is unique.

Proof. Suppose to the contrary, $\exists e' \neq e, \text{ s.t. } g * e' = e' * g = g$. Then, $e * g = g \Rightarrow e * e' = e'$; $g * e' = g \Rightarrow e * e' = e$. Therefore, $e * e' = e' = e$. Contradiction. \square

Remark 1.2. $g^{-1} * g = e$.

Proof. Suppose $h * g = e$, we want to show $h = g^{-1}$.
 $h = h * e = h * (g * g^{-1}) = (h * g) * g^{-1} = e * g^{-1} = g^{-1}$. \square

Remark 1.3. $\forall g$, its inverse g^{-1} is unique.

Proof. Suppose $\exists h \neq g^{-1}, \text{ s.t. } g * h = e$.
 $h = e * h = (g^{-1} * g) * h = g^{-1} * (g * h) = g^{-1} * e = g^{-1}$. Contradiction. \square

Remark 1.4. If h is the inverse of g , i.e., $h = g^{-1}$, then g is the inverse of h , i.e., $g = h^{-1}$.

Proof. $h^{-1} = e * h^{-1} = (g * h) * h^{-1} = g * (h * h^{-1}) = g * e = g$. \square

Remark 1.5 (Cancellation Law). Let $\forall a, b, c \in G$. If $a * b = a * c$, then $b = c$. If $b * a = c * a$, then $b = c$.

Proof. $b = e * b = (a^{-1} * a) * b = a^{-1} * (a * b) = a^{-1} * (a * c) = (a^{-1} * a) * c = e * c = c$. \square

Definition 1.2 (Abelian Group). An abelian group $(G, *)$ is a group whose law of composition is commutative. That is, $\forall a, b \in G, a * b = b * a$.

Example 1.1. *Abelian Groups:*

1. \mathbb{Z}^+ : integers, with addition.
2. \mathbb{R}^+ : real numbers, with addition.
3. \mathbb{R}^\times : nonzero real numbers, with multiplication.
4. $\mathbb{C}^+, \mathbb{C}^\times$: complex numbers, with addition or multiplication (nonzero).

Example 1.2. *Non-Abelian Groups:*

1. (General Linear Group)
 $GL_n(\mathbb{R})$ (or $GL_n(\mathbb{C})$) = $\{n \times n \text{ real (or complex) matrices } A \text{ with } \det A \neq 0\}$.
2. (Symmetric Group) S_n = group of permutations of $\{1, \dots, n\}$. The order of the group is $n!$.

1.2 Subgroups

Definition 1.3 (Subgroup). A subset H of a group G is called a subgroup if it has the following properties:

1. Closure: If $a \in H$ and $b \in H$, then $a * b \in H$.
2. Identity: $e \in H$.
3. Inverses: If $a \in H$, then $a^{-1} \in H$.

Remark 1.6. Associativity is automatic.

Remark 1.7. Every group has two obvious subgroups:

1. the whole group $(G, *)$;
2. $(e, *)$.

Definition 1.4 (Proper Subgroup). A subgroup is said to be a proper subgroup if it is not $(G, *)$ or $(e, *)$.

Example 1.3. *Proper Subgroups:*

1. The set T of invertible upper triangular 2×2 matrices

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} (a, d \neq 0)$$

is a subgroup of the general linear group $GL_n(\mathbb{R})$.

2. The set of complex numbers of absolute value 1 – the set of points on the unit circle in the complex plane – is a subgroup of \mathbb{C}^\times .
3. The subset $b\mathbb{Z} = \{n \in \mathbb{Z} \mid n = bk \text{ for some } k \in \mathbb{Z}\}$ is a subgroup of \mathbb{Z}^+ . Moreover, every subgroup H of \mathbb{Z}^+ is of the type $H = b\mathbb{Z}$ for some integer b .

Proposition 1.1. *Let a, b be integers, not both 0, and let d be the positive integer which generates the subgroup $a\mathbb{Z} + b\mathbb{Z}$. Then,*

1. *d can be written in the form $d = ar + bs$ for some integer r and s .*
2. *d divides a and b .*
3. *If integer e divides a and b , it also divides d .*

Definition 1.5 (Order of a Group). *The order of any group G is the number of its elements.*

$$|G| = \text{number of elements of } G.$$

Definition 1.6 (Order of an Element). *An element of a group is said to have order m (possibly infinity) if the cyclic subgroup it generates has order m . That is, m is the smallest positive integer with the property $x^m = 1$ or, if the order is infinite, that $x^m \neq 1$ for all $m \neq 0$.*

Example 1.4. *For $GL_n(\mathbb{R})$*

1. $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ *is an element of order 6.*
2. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ *has infinite order, since $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.*

Example 1.5. *Non-cyclic Groups:*

1. *The Klein four group $V = \langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle$ is the simplest group which is not cyclic.*
2. *The quaternion group H is another example of a small subgroup of $GL_n(\mathbb{C})$ which is not cyclic. It consists of the eight matrices $H = \{\pm 1, \pm i, \pm j, \pm k\}$, where*

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

1.3 Isomorphisms

Definition 1.7 (Isomorphic). *Let G and G' be two groups. We want to say that they are isomorphic if all properties of the group structure of G hold for G' as well, and conversely. Denote $G \approx G'$.*

Definition 1.8 (Isomorphism). *An isomorphism φ from $(G, *)$ to $(G', *')$ is a bijective map which is compatible with the laws of composition. That is $\varphi(a * b) = \varphi(a) *' \varphi(b)$.*

Example 1.6. *Isomorphisms:*

1. *Let $C = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}$ be an infinite cyclic group. Then the map $\varphi : \mathbb{Z}^+ \rightarrow C$ defined by $\varphi(n) = a^n$ is an isomorphism.*
2. *Let $G = \{1, x, x^2, \dots, x^{n-1}\}$ and $G' = \{1, y, y^2, \dots, y^{n-1}\}$ be two cyclic groups, generated by elements x, y of the same order. Then the map which sends x^i to y^i is an isomorphism: Two cyclic groups of the same order are isomorphic.*

Definition 1.9 (Isomorphism Class). The groups isomorphic to a given group G form what is called the isomorphism class of G , and any two groups in an isomorphism class are isomorphic.

Definition 1.10 (Automorphism). A map $\varphi : G \rightarrow G$ is called an automorphism of G .

Remark 1.8. The identity map is an automorphism.

Remark 1.9. The most important example of automorphism is conjugation: Let $b \in G$ be a fixed element. Then conjugation by b is the map φ from G to itself defined by

$$\varphi(x) = bxb^{-1}.$$

This is an automorphism. Any noncommutative group has some nontrivial conjugations, and so it has nontrivial automorphisms.

Definition 1.11 (Conjugate). Two elements a, a' of a group G are called conjugate if $a' = bab^{-1}$ for some $b \in G$.

Remark 1.10. The conjugate behaves in much the same way as the element a itself; for example, it has the same order in the group. This follows from the fact that it is the image of a by an automorphism.

1.4 Homomorphisms

Definition 1.12 (Homomorphism). Let G, G' be groups. A homomorphism $\varphi : G \rightarrow G'$ is any map satisfying $\varphi(a * b) = \varphi(a) *' \varphi(b)$.

Remark 1.11. Note that φ does not need to be bijective.

Example 1.7. Homomorphisms:

1. the determinant function $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$.
2. the sign of a permutation $\text{sign} : S_n \rightarrow \{\pm 1\}$.
3. the map $\varphi : \mathbb{Z}^+ \rightarrow G$ defined by $\varphi(n) = a^n$, where a is a fixed element of G .
4. the inclusion map: $i : H \rightarrow G$ of a subgroup H into a group G , defined by $i(x) = x$.

Remark 1.12. A group homomorphism $\varphi : G \rightarrow G'$ carries the identity to the identity, and inverses to inverses.

Proof. $\varphi(e) = \varphi(e * e) = \varphi(e) *' \varphi(e)$; $\varphi(a^{-1}) *' \varphi(a) = \varphi(a^{-1} * a) = \varphi e = e'$. □

Definition 1.13 (Image). The image of a homomorphism $\varphi : G \rightarrow G'$ is the image of the map

$$\text{im } \varphi = \{x \in G' \mid x = \varphi(a) \text{ for some } a \in G\}.$$

Definition 1.14 (Kernel). The kernel of φ is the set of elements of G which are mapped to the identity in G' :

$$\ker \varphi = \{a \in G \mid \varphi(a) = e'\}.$$

Remark 1.13. The kernel is a subgroup of G .

Example 1.8. Kernels:

1. The kernel of determinant homomorphism is called the special linear group

$$SL_n(\mathbb{R}) = \{\text{real } n \times n \text{ matrices } A \mid \det A = 1\}.$$

2. The kernel of the sign homomorphism is called the alternating group

$$A_n = \{\text{even permutations}\}.$$

Definition 1.15 (Normal Subgroup). A subgroup N of a group G is called a normal subgroup if it has the following property: For every $a \in N$ and every $b \in G$, the conjugate $bab^{-1} \in N$.

Remark 1.14. The kernel of a homomorphism is a normal subgroup.

Proof. $\varphi(bab^{-1}) = \varphi(b)\varphi(a)\varphi(b^{-1}) = \varphi(b)e\varphi(b)^{-1} = e'.$ □

Remark 1.15. Any subgroup of an abelian group G is normal.

Definition 1.16 (Center of a Group). The center of a group G , sometimes denoted by Z or by $Z(G)$, is the set of elements which commute with every element of G :

$$Z = \{z \in G \mid zx = xz \text{ for all } x \in G\}.$$

Remark 1.16. The center of any group is a normal subgroup of the group.

Example 1.9. The center of $GL_n(\mathbb{R})$ is the group of scalar matrices, that is, those of the form $c \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

1.5 Equivalence Relations and Partitions

Definition 1.17 (Equivalence Relation). An equivalence relation on S is a relation which holds between certain elements of S . Denoted as $a \sim b$. An equivalence relation is required to be:

1. transitive: If $a \sim b$ and $b \sim c$, then $a \sim c$.
2. symmetric: If $a \sim b$, then $b \sim a$.
3. reflexive: $a \sim a$ for all $a \in S$.

Definition 1.18 (Equivalence Class). The equivalence class of a is

$$C_a = \{b \in S \mid a \sim b\}.$$

Remark 1.17. If C_a and C_b have an element d in common. Then $C_a = C_b$.

Proposition 1.2. Let $\varphi : G \rightarrow G'$ be a group homomorphism with kernel N , and let a, b be elements of G . Then $\varphi(a) = \varphi(b)$ if and only if $b = an$ for some element $n \in N$, or equivalently, if $a^{-1}b \in N$.

Proof. Suppose $\varphi(a) = \varphi(b)$. Then $\varphi(a)^{-1}\varphi(b) = e'$. Since φ is a homomorphism, $\varphi(a^{-1}b) = e'$. By definition of the kernel, $a^{-1}b \in N$. Conversely, if $b = an$ for some $n \in N$. Then $\varphi(b) = \varphi(a)\varphi(n) = \varphi(a)e' = \varphi(a)$. \square

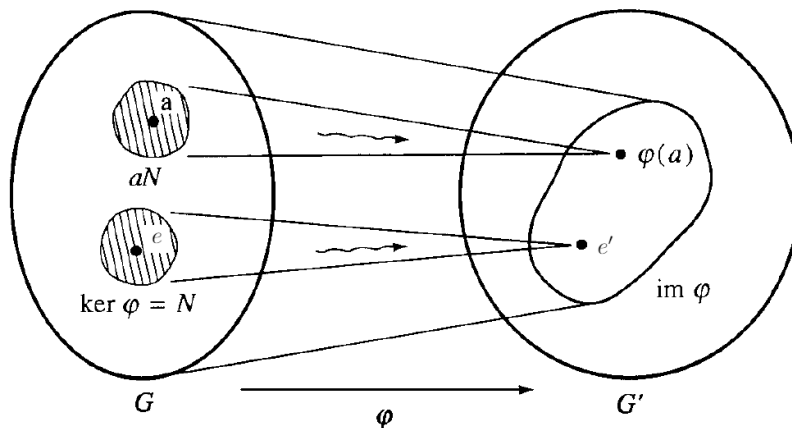


Figure 1: A schematic diagram of a group homomorphism.

Definition 1.19 (Coset). The set of elements of the form an is denoted by aN and is called a coset of N in G :

$$aN = \{g \in G \mid g = an \text{ for some } n \in N\}.$$

1.6 Cosets

One can define cosets for any subgroup H of a group G , not only for the kernel of a homomorphism.

Definition 1.20 (Left Coset). A left coset is a subset of the form

$$aH = \{ah \mid h \in H\}.$$

Remark 1.18. The cosets are equivalence classes.

Remark 1.19. The left cosets of a subgroup partition the group.

Remark 1.20. Each coset aH has the same number of elements as H does.

Definition 1.21 (Index). The number of left cosets of a subgroup is called the index of H in G and is denoted by

$$[G : H].$$

Theorem 1.1 (Lagrange's Theorem). Let G be a finite group, and let H be a subgroup of G . The order of H divides the order of G .

Corollary 1.1. Let $\varphi : G \rightarrow G'$ be a homomorphism of finite groups. Then

$$|G| = |\ker \varphi| \cdot |\operatorname{im} \varphi|.$$

Definition 1.22 (Right Coset). A right coset is a subset of the form

$$Ha = \{ha \mid h \in H\}.$$

Remark 1.21. *Right cosets need not be the same as left cosets.*

Proposition 1.3. *A subgroup H of a group G is normal if and only if every left coset is also a right coset. If H is normal, then $aH = Ha$ for every $a \in G$.*

Proof. Suppose that H is normal. For any $h \in H$, and any $a \in G$,

$$ah = (aha^{-1})a \in Ha.$$

This shows that $aH \subset Ha$. Similarly, $Ha \subset aH$. So, $aH = Ha$. Conversely, suppose that H is not normal. Then $\exists h \in H$ and $a \in G$ s.t. $aha^{-1} \notin H$. Then $ah \in aH$ and $ah \notin Ha$. So, $aH \neq Ha$. However, $a \in aH \cap Ha$. Therefore, aH can't be in some other right coset. This shows that the partition into left cosets is not the same as the partition into right cosets. \square

1.7 Restriction of a Homomorphism to a Subgroup

Proposition 1.4. *The intersection $K \cap H$ of two subgroups is a subgroup of H . If K is a normal subgroup of G , then $K \cap H$ is a normal subgroup of H .*

Remark 1.22. *If $|H|$ and $|K|$ have no common factor, then $K \cap H = \{1\}$.*

Remark 1.23. *Suppose that a homomorphism $\varphi : G \rightarrow G'$ is given and that H is a subgroup of G . Then we may restrict φ to H :*

$$\varphi|_H : H \rightarrow G'.$$

The kernel of $\varphi|_H$ is

$$\ker \varphi|_H = (\ker \varphi) \cap H.$$

Proposition 1.5. *Let $\varphi : G \rightarrow G'$ be a homomorphism, and let H' be a subgroup of G' . Denote the inverse image $\varphi^{-1}(H') = \{x \in G \mid \varphi(x) \in H'\}$ by \tilde{H} .*

1. \tilde{H} is a subgroup of G .
2. If H' is a normal subgroup of G' , then \tilde{H} is a normal subgroup of G .
3. \tilde{H} contains $\ker \varphi$.
4. The restriction of φ to \tilde{H} defines a homomorphism $\tilde{H} \rightarrow H'$, whose kernel is $\ker \varphi$.

Proof. We verify the conditions for a subgroup:

1. Closure: Suppose $x, y \in \tilde{H}$, then $\varphi(x)$ and $\varphi(y)$ are in H' . Since H' is a subgroup, $\varphi(x)\varphi(y) \in H'$. Since φ is a homomorphism, $\varphi(x)\varphi(y) = \varphi(xy) \in H'$. So, $xy \in \tilde{H}$.
2. Identity: $e \in \tilde{H}$ since $\varphi(e) = e' \in H'$.
3. Inverses: Suppose $x \in \tilde{H}$, so that $\varphi(x) \in H'$, then $\varphi(x)^{-1} \in H'$. Since φ is a homomorphism, $\varphi(x)^{-1} = \varphi(x^{-1})$. Thus, $x^{-1} \in \tilde{H}$.

Suppose that H' is a normal subgroup, and let $x \in \tilde{H}$ and $g \in G$. Then $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1}$, and $\varphi(x) \in H'$. Therefore, $\varphi(gxg^{-1}) \in H'$, and this shows that $gxg^{-1} \in \tilde{H}$.

Next, \tilde{H} contains $\ker \varphi$ because if $x \in \ker \varphi$ then $\varphi(x) = e'$, and $e' \in H'$. So $x \in \varphi^{-1}(H')$. \square

Example 1.10. *Consider the determinant homomorphism: $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$. The set P of positive real numbers is a subgroup of \mathbb{R} , and its inverse image is the set of invertible $n \times n$ matrices with positive determinant, which is a normal subgroup of $GL_n(\mathbb{R})$.*

1.8 Products of Groups

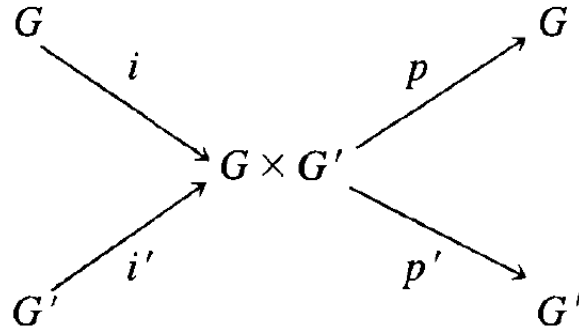
Definition 1.23 ($G \times G'$). We define multiplication of pairs by the rule

$$(a, a'), (b, b') \mapsto (ab, a'b'),$$

for $a, b \in G$ and $a', b' \in G'$. The pair (e, e') is an identity. And $(a, a')^{-1} = (a^{-1}, a'^{-1})$. The group thus obtained is called the product of G and G' and is denoted by $G \times G'$.

Remark 1.24. The order of $G \times G'$ is the product of the orders of G and G' .

Remark 1.25. The product group is related to the two factors G, G' in a simple way, which can be summed up in terms of some homomorphisms:



defined by

$$\begin{aligned} i(x) &= (x, 1), i'(x') = (1, x'); \\ p(x, x') &= x, p'(x, x') = x'. \end{aligned}$$

The maps i, i' are injective and the maps p, p' are surjective.

$$\ker p = 1 \times G'$$

and

$$\ker p' = G \times 1.$$

These maps are called projections.

Proposition 1.6 (The mapping property of products). Let H be any group. The homomorphisms $\Phi : H \rightarrow G \times G'$ are in bijective correspondence with pairs (φ, φ') of homomorphisms

$$\varphi : H \rightarrow G, \varphi' : H \rightarrow G'.$$

The kernel of Φ is the intersection $(\ker \varphi) \cap (\ker \varphi')$.

Proof. Given a pair (φ, φ') of homomorphisms, we define the corresponding homomorphism

$$\Phi : H \rightarrow G \times G'$$

by the rule $\Phi(h) = (\varphi(h), \varphi'(h))$. Conversely, given Φ , we obtain φ and φ' by composition with the projections, as

$$\varphi = p\Phi, \varphi' = p'\Phi.$$

Obviously, $\Phi(h) = (e, e')$ if and only if $\varphi(h) = e$ and $\varphi'(h) = e'$, which shows that $\ker \Phi = (\ker \varphi) \cap (\ker \varphi')$. \square

Example 1.11. A cyclic group C_6 of order 6 is isomorphic to the product $C_2 \times C_3$ of cyclic groups of orders 2 and 3.

Proposition 1.7. Let r, s be integers with no common factor. A cyclic group of order rs is isomorphic to the product of a cyclic group of order r and a cyclic group of order s .

Definition 1.24. Let A and B be subsets of a group G . Then we denote the set of products of elements of A and B by

$$AB = \{x \in G \mid x = ab \text{ for some } a \in A \text{ and } b \in B\}.$$

Proposition 1.8. Let H and K be subgroups of a group G .

1. If $H \cap K = e$, the product map $p : H \times K \rightarrow G$ defined by $p(h, k) = hk$ is injective. Its image is the subset HK .
2. If either H or K is a normal subgroup of G , then the product sets HK and KH are equal, and HK is a subgroup of G .
3. If H and K are normal, $H \cap K = e$, and $HK = G$, then G is isomorphic to the product group $H \times K$.

Proof. 1. Let $(h_1, k_1), (h_2, k_2)$ be elements of $H \times K$ such that $h_1 k_1 = h_2 k_2$. multiplying both sides of this equation on the left by h_1^{-1} and on the right by k_2^{-1} , we find $k_1 k_2^{-1} = h_1^{-1} h_2$. Since $H \cap K = e$, $k_1 k_2^{-1} = h_1^{-1} h_2 = e$, hence $h_1 = h_2$ and $k_1 = k_2$. This shows that p is injective.

2. Suppose that H is a normal subgroup of G , and let $h \in H$ and $k \in K$. Note that $kh = (khk^{-1})k$. Since H is normal, $khk^{-1} \in H$. Therefore $kh \in HK$, which shows that $KH \subset HK$. The proof of the other inclusion is similar. The fact that HK is a subgroup now follows easily. For closure under multiplication, note that in a product $(hk)(h'k') = h(kh')k'$, the middle term kh' is in $KH = HK$, say $kh' = h''k''$. Then $hkh'k' = (hh'')(k''k') \in HK$. Closure under inverses is similar: $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. And of course, $e = ee \in HK$. Thus HK is a subgroup. The proof is similar in the case that K is normal.

3. Assume that both subgroups are normal and that $H \cap K = e$. Consider the product $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$. Since K is a normal subgroup, the left side is in K . Since H is normal, the right side is in H . Thus this product is the intersection $H \cap K$, i.e., $hkh^{-1}k^{-1} = e$. Therefore $hk = kh$. This being known, the fact that p is a homomorphism follows directly: In the group $H \times K$, the product rule is $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$, and this element corresponds to $h_1 h_2 k_1 k_2 \in G$, while in G the products $h_1 k_1$ and $h_2 k_2$ multiply as $h_1 k_1 h_2 k_2$. Since $h_2 k_1 = k_1 h_2$, the products are equal. Part (1) shows that p is injective, and the assumption that $HK = G$ shows that p is surjective.

□

Remark 1.26. It is important to note that the product map $p : H \times K \rightarrow G$ will not be a group homomorphism unless the two subgroups commute with each other.

1.9 Quotient Groups

Lemma 1.1. *Let N be a normal subgroup of a group G . Then the product of two cosets aN , bN is again a coset, in fact*

$$(aN)(bN) = abN.$$

Proof. Note that $Nb = bN$, and since N is a subgroup $NN = N$.

$$(aN)(bN) = a(Nb)N = a(bN)N = abNN = abN.$$

□

Theorem 1.2. *With the law of composition, $\bar{G} = G/N$ is a group, and the map $\pi : G \rightarrow \bar{G} = G/N$ sending $a \mapsto \bar{a} = aN$ is a homomorphism with kernel N .*

Corollary 1.2. *Every normal subgroup of a group G is the kernel of a homomorphism.*

Theorem 1.3 (First Isomorphism Theorem). *Let $\varphi : G \rightarrow G'$ be a surjective group homomorphism, and let $N = \ker \varphi$. Then G/N is isomorphic to G' by the map $\bar{\varphi}$ which sends the cosets $\bar{a} = aN$ to $\varphi(a)$:*

$$\bar{\varphi}(\bar{a}) = \varphi(a).$$

Example 1.12. 1. *The absolute value map $\mathbb{C}^\times \rightarrow \mathbb{R}^\times$ maps the nonzero complex numbers to the positive real numbers, and its kernel is the unit circle U . So the quotient group \mathbb{C}^\times/U is isomorphic to the multiplicative group of positive real numbers.*

2. *The determinant is a surjective homomorphism $GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$, whose kernel is the special linear group $SL_n(\mathbb{R})$. So the quotient group $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ is isomorphic to \mathbb{R}^\times .*